(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10004403 A**

(43) Date of publication of application: **06.01.98**

(51) Int. Cl **H04L 9/16**
G06F 12/14
G06K 17/00
H04L 9/08

(21) Application number: **08155696**

(22) Date of filing: **17.06.96**

(71) Applicant: **N T T DATA TSUSHIN KK**

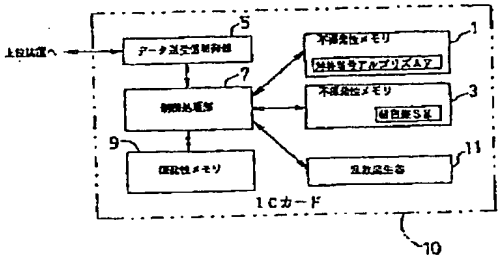
(72) Inventor: **KOBAYASHI TAKAFUMI**
SUGANO NAOYUKI

(54) ENCRYPTION DEVICE, DECODE DEVICE AND METHOD THEREFOR

(57) Abstract:

PROBLEM TO BE SOLVED: To make it hard to illegally decode a secret key by updating a temporary key as a secret key in every preprocessing or postprocessing in encryption and decode processing.

SOLUTION: A control processing part 7 reads symmetrical cipher algorithm F from 1st nonvolatile memory 1, makes the algorithm F process a secret key SK and a random number which are stored in volatile memory 9 and stores the information generated from this processed result as a key for temporary cipher processing, i.e., a temporary key in the memory 9. Next, the part 7 makes the algorithm F process a clear text and the temporary key which are stored in the memory 9 and stores this processed result as a cipher text in the memory 9. When the cipher text is created in this way, the part 7 reads the temporary key stored in the memory 9, rewrites and updates a secret key which is stored in 2nd nonvolatile memory 3 with this temporary key and prepares for the next encryption processing.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平10－4403

(43)公開日　平成10年(1998) 1月6日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/16			Ｈ０４Ｌ　9/00	６４３	
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｂ	
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｅ	
Ｈ０４Ｌ　9/08			Ｈ０４Ｌ　9/00	６０１Ｃ	

審査請求　未請求　請求項の数７　ＯＬ　（全 10 頁）

(21)出願番号　特願平8－155696

(22)出願日　平成８年(1996) ６月17日

(71)出願人　000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目３番３号

(72)発明者　小林　孝文
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　菅野　直行
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

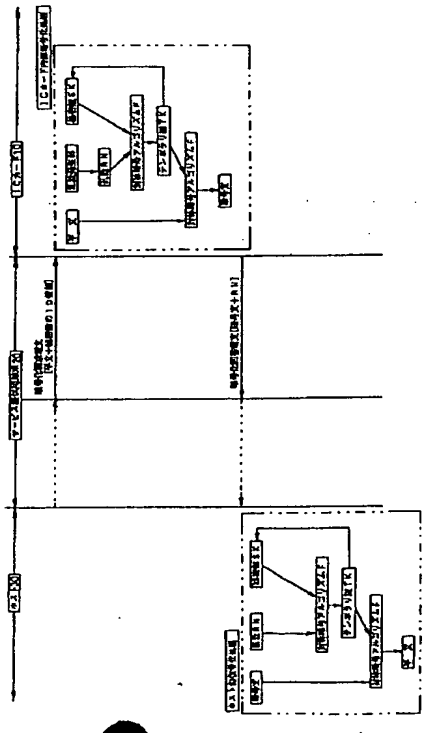
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　暗号化装置、復号化装置およびその方法

(57)【要約】

【課題】　暗号化処理または復号化処理の都度、秘密鍵を更新し、秘密鍵の不正な解読を困難にした暗号化装置、復号化装置およびその方法を提供する。

【解決手段】　乱数ＲＮおよび秘密鍵ＳＫを対称暗号アルゴリズムＦにより処理してテンポラリ鍵ＴＫを生成し、該テンポラリ鍵ＴＫおよび平文または暗号文を対称暗号アルゴリズムにより処理して暗号文または平文を生成するとともに、秘密鍵ＳＫをテンポラリ鍵ＴＫで更新し、次の暗号化処理または復号化処理に備えている。



【特許請求の範囲】

【請求項１】　秘密鍵および乱数を対称暗号アルゴリズムにより処理して一時鍵を生成し、この一時鍵および暗号化すべき平文または復号化すべき暗号文を当該対象暗号アルゴリズムによって処理して暗号文または平文を生成する方法であって、前記一時鍵を暗号化処理および復号化処理における処理前または処理後に、その都度、秘密鍵として更新することを特徴とする暗号化復号化方法。

【請求項２】　暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、
乱数を発生する乱数発生手段と、
暗号処理用の秘密鍵を格納している秘密鍵格納手段と、
対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、
前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、
前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数発生手段からの乱数および前記秘密鍵を処理し、暗号処理用の一時鍵を生成する一時鍵生成手段と、
前記平文および前記一時鍵を前記対称暗号アルゴリズムによって処理し、暗号文を生成する暗号文生成手段と、
前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを特徴とする暗号化装置。

【請求項３】　復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、
復号処理用の秘密鍵を格納している秘密鍵格納手段と、
対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、
対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数および秘密鍵格納手段に格納されている秘密鍵を処理し、復号処理用の一時鍵を生成する一時鍵生成手段と、
前記暗号文および前記一時鍵を前記対称暗号アルゴリズムによって処理し、平文を生成する平文生成手段と、
前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを特徴とする復号化装置。

【請求項４】　暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、
乱数を発生する乱数発生手段と、
暗号処理用の秘密鍵を格納している秘密鍵格納手段と、
対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、
前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、
前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記平文および前記秘密鍵を処理し、暗号文を生成する暗号生成手段と、
前記対称暗号アルゴリズムにより前記乱数発生手段からの乱数および前記秘密鍵を処理し、一時鍵を生成する一時鍵生成手段と、
前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを特徴とする暗号化装置。

【請求項５】　復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、
復号処理用の秘密鍵を格納している秘密鍵格納手段と、
対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、
対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記暗号文および秘密鍵格納手段に格納されている秘密鍵を処理し、平文を生成する平文生成手段と、
前記乱数および前記秘密鍵を前記対称暗号アルゴリズムによって処理し、一時鍵を生成する一時鍵生成手段と、
前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを特徴とする復号化装置。

【請求項６】　暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、
乱数を発生する乱数発生手段と、
暗号処理用の秘密鍵を格納している秘密鍵格納手段と、
対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、
前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、
前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数発生手段からの乱数および前記秘密鍵を処理し、一時鍵を生成する一時鍵生成手段と、
前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段と、
前記平文および前記更新手段で更新された秘密鍵を前記対称暗号アルゴリズムによって処理し、暗号文を生成する暗号文生成手段とを有することを特徴とする暗号化装置。

【請求項７】　復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、
復号処理用の秘密鍵を格納している秘密鍵格納手段と、
対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、
対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数および秘密鍵格納手段に格納されている

秘密鍵を処理し、復号処理用の一時鍵を生成する一時鍵生成手段と、
前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段と、
前記平文および前記更新手段を更新された秘密鍵を前記対称暗号アルゴリズムによって処理し、平文を生成する平文生成手段とを有することを特徴とする復号化装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばＩＣカード内で対称暗号アルゴリズムと秘密鍵を用いて行われる暗号化処理または復号化処理において秘密鍵の不正な解読を困難にすべく暗号化処理または復号化処理の都度秘密鍵を更新する暗号化装置、復号化装置およびその方法に関する。
【０００２】
【従来の技術】システム内で扱うデータの機密性を高めるために、例えばＩＣカードを用いてデータの暗号処理を行う場合、比較的短い時間で暗号処理が可能であるともとに、解読が比較的困難とされている対称暗号アルゴリズムおよび秘密鍵をＩＣカード内に格納しておき、ＩＣカード内でデータの暗号化処理を行う方式が有力視されている。
【０００３】このように、ＩＣカード内で対称暗号アルゴリズムと秘密鍵を用いて暗号化処理を行う方式においても、最近のコンピュータ技術および暗号解読技術の進歩により、暗号文とこの暗号文の元となった生データである平文のペアをいくつか取得することにより、ＩＣカード内に格納されている秘密鍵を外部ハッカー等により解読できる可能性があることが発表されている。
【０００４】このような外部ハッカー等による秘密鍵の不正な解読をより困難にするために、対称暗号アルゴリズムをより複雑にしたり、またはＩＣカード内に格納された秘密鍵をあるタイミングにより、または暗号化処理を行う度に、システム側で新しい秘密鍵を生成してＩＣカードに送信し、今まで使用されていたＩＣカード内の秘密鍵を新しい秘密鍵で更新することが考えられている。
【０００５】
【発明が解決しようとする課題】上述したように、例えばＩＣカード内で対称暗号アルゴリズムおよび秘密鍵を用いて暗号化処理を行う方式において、外部ハッカー等による秘密鍵の不正な解読を防止するために考えられている方法のうち、対称暗号アルゴリズムをより複雑にする方法は、複雑なアルゴリズムを開発するために多くの時間とコストがかかるとともに、更に複雑なアルゴリズムの複雑性、すなわち解読困難性を評価するための時間とコストもかかるという問題に加えて、またアルゴリズムが複雑になればなるだけ、ＩＣカード内の処理時間が増大するという問題がある。
【０００６】また、システム側で新しい秘密鍵を生成し、ＩＣカードに送信して更新する方法は、どのタイミングで、すなわちどれくらいの時間をおいてシステム側で新しい秘密鍵を生成し、ＩＣカードに送信して更新すればよいのかを検証および保証することが困難であるという問題があるとともに、またシステム側で生成した新しい秘密鍵をＩＣカードに送信する際に、新しい秘密鍵を外部ハッカー等に盗まれる可能性があるが、これを防止し、安全にＩＣカードに送信するために、システム側で生成した新しい秘密鍵を更に別の秘密鍵で暗号化し、ＩＣカードに送信する必要があるなどのように処理が更に複雑になるという問題がある。
【０００７】本発明は、上記に鑑みてなされたもので、その目的とするところは、暗号化処理または復号化処理の都度、秘密鍵を更新し、秘密鍵の不正な解読を困難にした暗号化装置、復号化装置およびその方法を提供することにある。
【０００８】
【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、秘密鍵および乱数を対称暗号アルゴリズムにより処理して一時鍵を生成し、この一時鍵および暗号化すべき平文または復号化すべき暗号文を当該対称暗号アルゴリズムによって処理して暗号文または平文を生成する方法であって、前記一時鍵を暗号化処理および復号化処理における処理前または処理後に、その都度、秘密鍵として更新することを要旨とする。
【０００９】請求項１記載の本発明にあっては、対称暗号アルゴリズムにより一時鍵および平文または暗号文を処理して暗号文または平文を生成する暗号化処理または復号化処理の前または後において、その都度、一時鍵を秘密鍵として更新することで、システムで扱うデータの機密性を高めている。
【００１０】請求項２記載の本発明は、暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数発生手段からの乱数および前記秘密鍵を処理し、暗号処理用の一時鍵を生成する一時鍵生成手段と、前記平文および前記一時鍵を前記対称暗号アルゴリズムによって処理し、暗号文を生成する暗号文生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを要旨とする。
【００１１】請求項２記載の本発明にあっては、対称暗号アルゴリズムにより乱数発生手段からの乱数および秘

密鍵を処理して一時鍵を生成し、該一時鍵および平文を対称暗号アルゴリズムにより処理して暗号文を生成するとともに、秘密鍵格納手段に格納されている秘密鍵を一時鍵で更新し、次の暗号化処理に備えている。

【００１２】請求項３記載の本発明は、復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数および秘密鍵格納手段に格納されている秘密鍵を処理し、復号処理用の一時鍵を生成する一時鍵生成手段と、前記暗号文および前記一時鍵を前記対称暗号アルゴリズムによって処理し、平文を生成する平文生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを要旨とする。

【００１３】請求項３記載の本発明にあっては、対称暗号アルゴリズムにより暗号文の生成に用いられた秘密鍵乱数および暗号文の生成に用いられた乱数を処理して一時鍵を生成し、該一時鍵および暗号文を対称暗号アルゴリズムにより処理して平文を生成するとともに、秘密鍵格納手段に格納されている秘密鍵を一時鍵で更新し、次の復号化処理に備えている。

【００１４】また、請求項４記載の本発明は、暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記平文および前記秘密鍵を処理し、暗号文を生成する暗号生成手段と、前記対称暗号アルゴリズムにより前記乱数発生手段からの乱数および前記秘密鍵を処理し、一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを要旨とする。

【００１５】請求項４記載の本発明にあっては、対称暗号アルゴリズムにより平文および秘密鍵を処理して暗号文を生成するとともに、対称暗号アルゴリズムにより乱数および秘密鍵を処理して一時鍵を生成し、秘密鍵格納手段に格納されている秘密鍵を該一時鍵で更新し、次の暗号化処理に備えている。

【００１６】請求項５記載の本発明は、復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記暗号文および秘密鍵格納手段に格納されている秘密鍵を処理し、平文を生成する平文生成手段と、前記乱数および前記秘密鍵を前記対称暗号アルゴリズムによって処理し、一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを要旨とする。

【００１７】請求項５記載の本発明にあっては、対称暗号アルゴリズムにより暗号文および秘密鍵を処理して平文を生成するとともに、対称暗号アルゴリズムにより暗号文の生成に用いられた秘密鍵乱数および暗号文の生成に用いられた乱数を処理して一時鍵を生成し、秘密鍵格納手段に格納されている秘密鍵を該一時鍵で更新し、次の復号化処理に備えている。

【００１８】更に、請求項６記載の本発明は、暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数発生手段からの乱数および前記秘密鍵を処理し、一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段と、前記平文および前記更新手段で更新された秘密鍵を前記対称暗号アルゴリズムによって処理し、暗号文を生成する暗号文生成手段とを有することを要旨とする。

【００１９】請求項６記載の本発明にあっては、対称暗号アルゴリズムによって乱数および秘密鍵を処理して一時鍵を生成し、この一時鍵で秘密鍵を更新するとともに、この更新された秘密鍵および平文を対称暗号アルゴリズムによって処理して暗号文を生成している。

【００２０】請求項７記載の本発明は、復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数および秘密鍵格納手段に格納されている秘密鍵を処理し、復号処理用の一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段と、前記平文および前記更新手段を更新された秘密鍵を前記対称暗号アルゴリズムによって処理し、平文を生成する平文生成手段とを有することを要旨とする。

【００２１】請求項７記載の本発明にあっては、対称暗号アルゴリズムによって暗号文の生成に用いられた秘密鍵乱数および暗号文の生成に用いられた乱数を処理して一時鍵を生成し、この一時鍵で秘密鍵を更新するとともに、この更新された秘密鍵および暗号文を対称暗号アルゴリズムによって処理して平文を生成している。

【００２２】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００２３】図１は、本発明の一実施形態に係わる暗号化復号化方法を実施するＩＣカードの構成を示すブロック図である。同図に示すＩＣカード１０は、対称暗号アルゴリズムおよび秘密鍵を用いて、外部の上位装置から送信される平文または暗号文をそれぞれ暗号化または復号化するものであり、対称暗号アルゴリズムおよび秘密鍵をそれぞれ格納している第１の不揮発性メモリ１および第２の不揮発性メモリ3を有する。また、ＩＣカード１０は、上位装置とデータの送受信を行うデータ送受信制御部５、ＩＣカード全体の動作を制御する制御処理部７、上位装置から受信した平文、秘密鍵のＩＤ情報、ＩＣカード１０の内部で生成した暗号文や一時データ等を記憶する揮発性メモリ９、および乱数を発生する乱数発生器１１を有する。

【００２４】次に、図２を参照して、ＩＣカード１０で平文を暗号化する場合の処理について説明する。図１のＩＣカード１０は、図２に示すように外部の上位装置としてサービス提供用端末２０を介してホスト３０に接続され、該ホスト３０からサービス提供用端末２０を介して送信される暗号化すべき平文および秘密鍵のＩＤ情報を暗号化要求電文とともにデータ送受信制御部５で受信する。

【００２５】データ送受信制御部５で受信された暗号化要求電文は、制御処理部７に供給されて解析される。制御処理部７は、受信した要求電文が暗号化要求電文であることを識別すると、該暗号化要求電文とともに送信されてきた平文およびＩＤ情報を揮発性メモリ９に格納する。ＩＤ情報は、ＩＣカード１０の第２の不揮発性メモリ３に格納されている暗号処理用の秘密鍵が第２の不揮発性メモリ３のどこに格納されているかを示す格納場所情報であり、該ＩＤ情報は第２の不揮発性メモリ３のアドレス情報でもよい。

【００２６】制御処理部７は、揮発性メモリ９に格納した秘密鍵のＩＤ情報に基づいて第２の不揮発性メモリ３内を検索し、暗号処理用の秘密鍵（以下、秘密鍵ＳＫとも称する）を第２の不揮発性メモリ３から読み出し、揮発性メモリ９に格納する。なお、このとき、第２の不揮発性メモリ３内の秘密鍵ＳＫ自体の消去は行わない。

【００２７】また、乱数発生器１１から乱数ＲＮを発生させ、この発生した乱数ＲＮを揮発性メモリ９に格納する。

【００２８】それから、制御処理部７は、第１の不揮発性メモリ１から対称暗号アルゴリズムＦを読み出し、揮発性メモリ９に格納した秘密鍵ＳＫおよび乱数ＲＮを対称暗号アルゴリズムＦによって処理させ、この処理の結果生成された情報ＴＫを一時的な暗号処理用の鍵、すなわち一時鍵ＴＫまたはテンポラリ鍵ＴＫとして揮発性メモリ９に格納する。

【００２９】次に、制御処理部７は、揮発性メモリ９に格納しておいた平文およびテンポラリ鍵ＴＫを対称暗号アルゴリズムＦにより処理させ、この処理結果を暗号文として揮発性メモリ９に格納する。

【００３０】このようにして暗号文が生成されると、制御処理部７は揮発性メモリ９に格納しておいたテンポラリ鍵ＴＫを読み出し、このテンポラリ鍵ＴＫで第２の不揮発性メモリ３に格納されている秘密鍵ＳＫを書き換えて更新し、次の暗号化処理に備える。

【００３１】また、制御処理部７は、揮発性メモリ９に格納した暗号文および乱数ＲＮを暗号化回答電文とともにサービス提供用端末２０を介してホスト３０に返送する。

【００３２】なお、図２には、ホスト３０における復号化処理が示されているが、この復号化処理では、ＩＣカード１０から返送された乱数ＲＮを用いてホスト３０内に記憶されている秘密鍵ＳＫを対称暗号アルゴリズムＦにより処理して、ＩＣカード１０において暗号化のために用いられたのと同じテンポラリ鍵ＴＫを生成し、このテンポラリ鍵ＴＫとＩＣカード１０からの暗号文を対称暗号アルゴリズムＦにより処理して平文に復号化している。また、秘密鍵ＳＫをテンポラリ鍵ＴＫで更新している。

【００３３】次に、図３を参照して、ＩＣカード１０で暗号文を復号化する場合の処理について説明する。ＩＣカード１０は、ホスト３０からサービス提供用端末２０を介して復号化要求電文とともに暗号文、秘密鍵のＩＤ情報、および乱数ＲＮを受信すると、ＩＣカード１０の制御処理部７は、受信信号を解析して、復号化要求電文であることを識別すると、暗号文、秘密鍵のＩＤ情報および乱数ＲＮを揮発性メモリ９に格納する。

【００３４】それから、揮発性メモリ９に格納したＩＤ情報で第２の不揮発性メモリ３を検索して、秘密鍵ＳＫを第２の不揮発性メモリ３から読み出し、この秘密鍵ＳＫおよびホスト３０から受信した乱数ＲＮを対称暗号アルゴリズムＦにより処理してホスト３０において暗号化のために用いられたのと同じテンポラリ鍵ＴＫを生成する。

【００３５】次に、該テンポラリ鍵ＴＫおよびホスト３０から受信した暗号文を対称暗号アルゴリズムＦにより処理し、平文を生成して揮発性メモリ９に格納する。それから、制御処理部７は揮発性メモリ９に格納しておいたテンポラリ鍵ＴＫを読み出し、このテンポラリ鍵ＴＫ

で第２の不揮発性メモリ３に格納されている秘密鍵ＳＫを書き換えて更新し、次の処理に備える。

【００３６】また、制御処理部７は、揮発性メモリ９に格納した平文を復号化回答電文としてサービス提供用端末２０を介してホスト３０に返送する。

【００３７】なお、図３には、ホスト３０における暗号化処理が示されているが、この暗号化処理の流れは図２に示したＩＣカード１０における暗号化処理と基本的に同じである。

【００３８】図４は、本発明の他の実施形態に係わる暗号化復号化方法におけるＩＣカードの別の暗号化処理を示す図である。

【００３９】上述した図２に示した実施形態における平文の暗号化処理においては対称暗号アルゴリズムＦにより平文とテンポラリ鍵ＴＫを処理して暗号文を生成していたのに対して、図４に示す本実施形態では、平文と秘密鍵ＳＫを対称暗号アルゴリズムＦにより処理して暗号文を生成している点が異なるものである。

【００４０】詳細に説明すると、ＩＣカード１０はホスト３０からサービス提供用端末２０を介して送信される暗号化すべき平文および秘密鍵のＩＤ情報を暗号化要求電文とともにデータ送受信制御部５で受信すると、暗号化要求電文が制御処理部７で解析され、平文およびＩＤ情報が揮発性メモリ９に格納される。

【００４１】制御処理部７は、揮発性メモリ９に格納した秘密鍵のＩＤ情報に基づいて第２の不揮発性メモリ３内を検索し、秘密鍵ＳＫを第２の不揮発性メモリ３から読み出し、揮発性メモリ９に格納する。

【００４２】次に、制御処理部７は、第１の不揮発性メモリ１から対称暗号アルゴリズムＦを読み出し、揮発性メモリ９に格納しておいた平文および秘密鍵ＳＫを対称暗号アルゴリズムＦにより処理させ、この処理結果を暗号文として揮発性メモリ９に格納する。

【００４３】また、乱数発生器１１から乱数ＲＮを発生させ、この発生した乱数ＲＮを揮発性メモリ９に格納する。

【００４４】それから、制御処理部７は、第１の不揮発性メモリ１から読み出した対称暗号アルゴリズムＦにより揮発性メモリ９に格納した秘密鍵ＳＫおよび乱数ＲＮを処理させ、一時鍵ＴＫであるテンポラリ鍵ＴＫを生成し、このテンポラリ鍵ＴＫで第２の不揮発性メモリ３に格納されている秘密鍵ＳＫを書き換えて更新し、次の暗号化処理に備える。

【００４５】また、制御処理部７は、揮発性メモリ９に格納した暗号文および乱数ＲＮを暗号化回答電文とともにサービス提供用端末２０を介してホスト３０に返送する。

【００４６】上述した図４におけるＩＣカード１０における暗号化処理では、最初にＩＣカード１０の第２の不揮発性メモリ３に格納されている秘密鍵ＳＫを用いて対称暗号アルゴリズムＦにより平文を処理して暗号化することを最初に行い、この後に該秘密鍵ＳＫを更新するように説明したが、この代わりに第２の不揮発性メモリ３に格納されている秘密鍵ＳＫを最初に更新し、この更新した秘密鍵ＳＫを用いて対称暗号アルゴリズムＦにより平文を処理して暗号化することも可能である。

【００４７】具体的には、ＩＣカード１０はホスト３０からサービス提供用端末２０を介して平文と秘密鍵のＩＤ情報を受信すると、このＩＤ情報で第２の不揮発性メモリ３から秘密鍵ＳＫを検索し、それから乱数発生器１１から乱数ＲＮを発生し、この乱数ＲＮと検索した秘密鍵ＳＫを対称暗号アルゴリズムＦにより処理してテンポラリ鍵ＴＫを生成し、このテンポラリ鍵ＴＫで第２の不揮発性メモリ３内の秘密鍵ＳＫを書き換えて更新する。

【００４８】それから、この更新した秘密鍵ＳＫを用いて対称暗号アルゴリズムＦにより平文を処理して暗号文を生成する。そして、制御処理部７は、この暗号文および乱数ＲＮを暗号化回答電文とともにサービス提供用端末２０を介してホスト３０に返送する。

【００４９】なお、図４にも、ホスト３０における復号化処理が示されているが、この復号化処理は図２に示したホスト３０における復号化処理においてテンポラリ鍵ＴＫの代わりに秘密鍵ＳＫを用いた点が異なるものである。

【００５０】

【発明の効果】以上説明したように、本発明によれば、システムで扱うデータの機密性を飛躍的に高めることができる上に、従来のように対称暗号アルゴリズムを複雑なアルゴリズムに変更したり、またはシステム側で秘密鍵を更新し、この更新した秘密鍵を更に別の秘密鍵で暗号化して送信するなどの複雑な処理を必要としないため、簡単かつ経済的にデータの機密性を向上することができ、外部ハッカーなどによる秘密鍵の不正な解読を適確に防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係わる暗号化復号化方法を実施するＩＣカードの構成を示すブロック図である。

【図２】図１に示すＩＣカードによる暗号化処理を示す図である。

【図３】図１に示すＩＣカードによる復号化処理を示す図である。

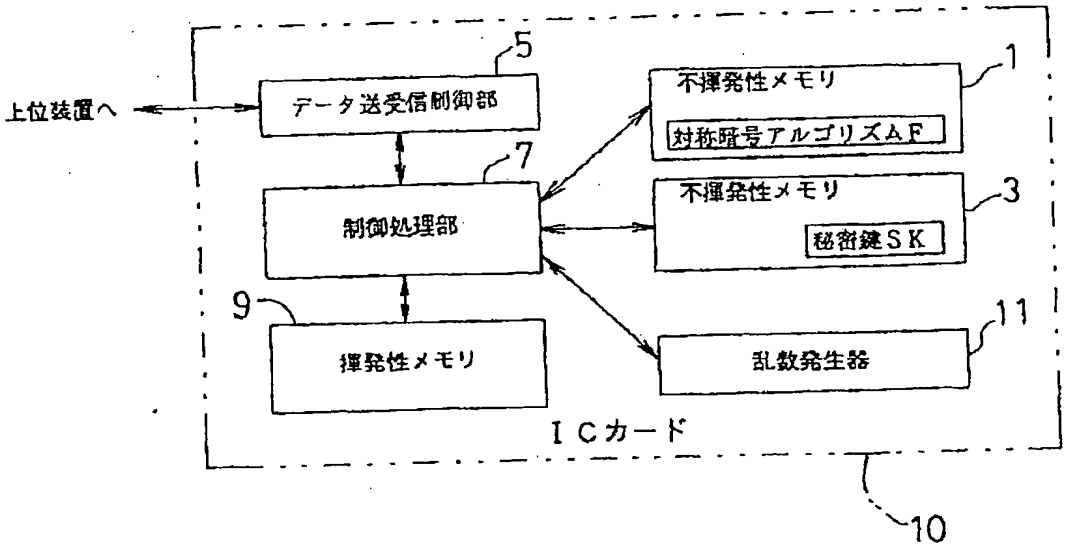
【図４】本発明の他の実施形態に係わる暗号化復号化方法を示す図であり、図１に示すＩＣカードの別の暗号化処理を示す図である。

【符号の説明】

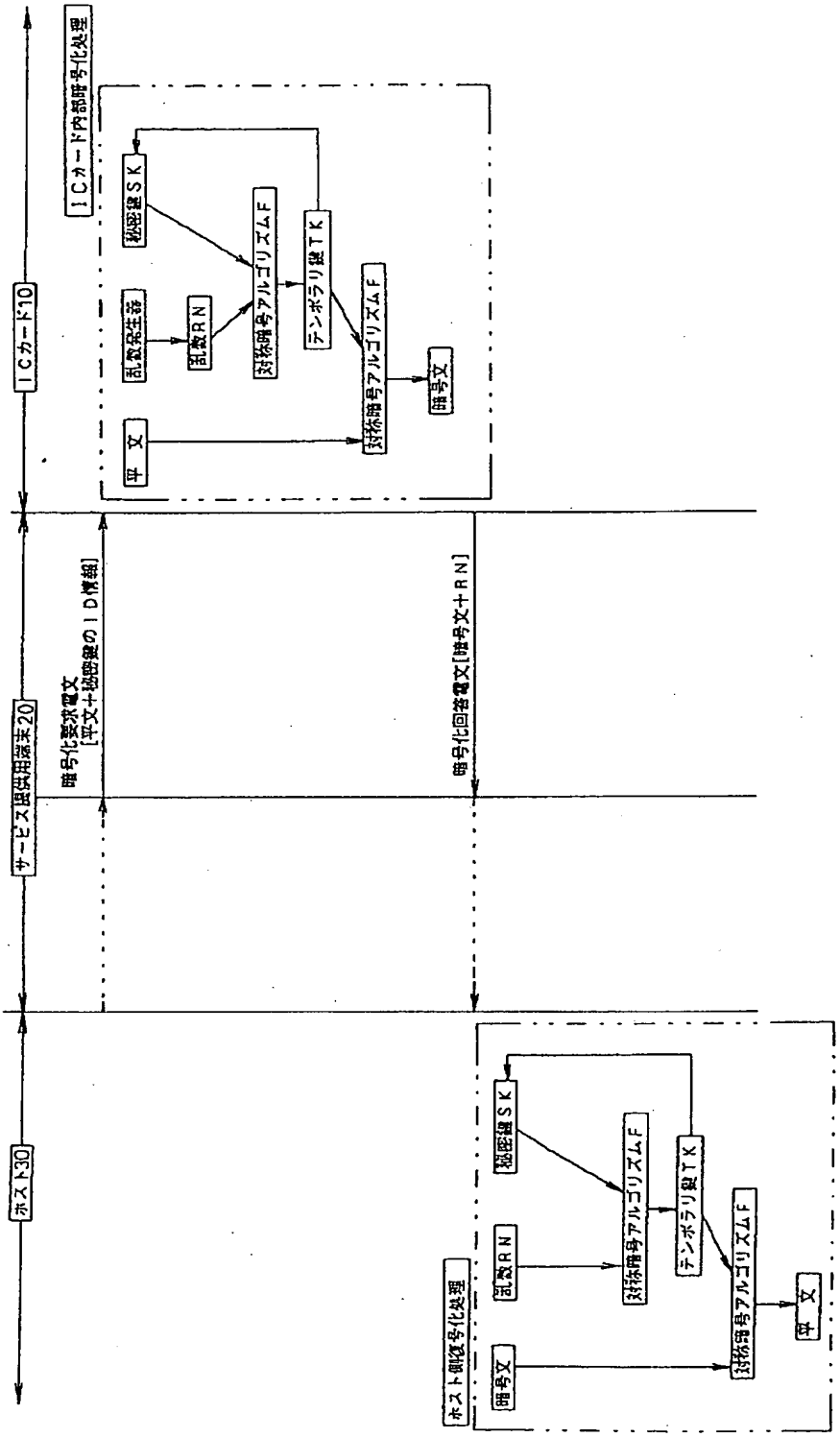
１　第１の不揮発性メモリ
３　第２の不揮発性メモリ
５　データ送受信制御部
７　制御処理部
９　揮発性メモリ

１０　ＩＣカード
１１　乱数発生器
２０　サービス提供用端末
３０　ホスト

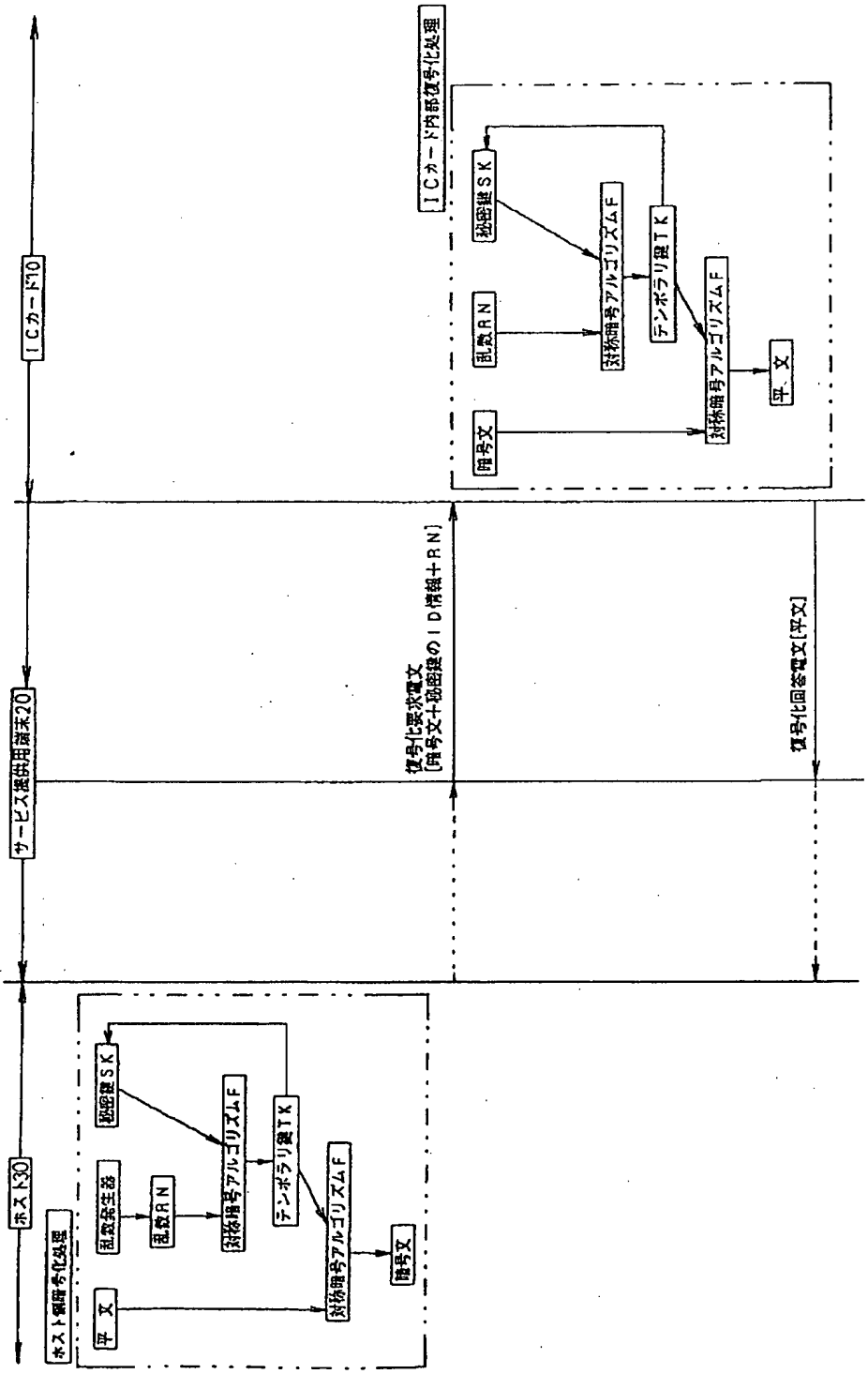
【図１】



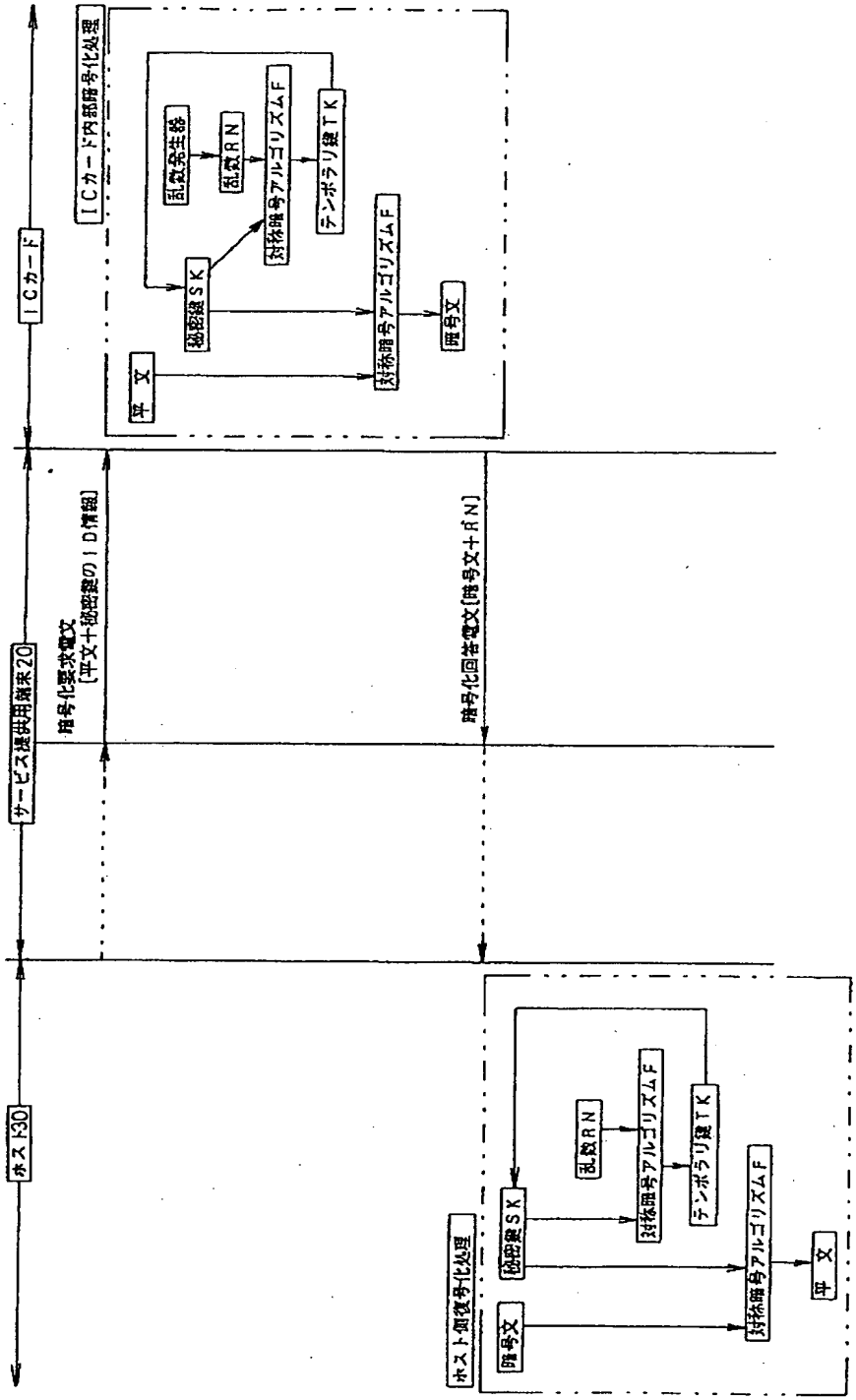
【図２】


ＩＣカード10
サービス提供用端末20
ホスト30
ＩＣカード内部暗号化処理
秘密鍵ＳＫ
乱数発生部
乱数ＲＮ
対称暗号アルゴリズムＦ
テンポラリ鍵ＴＫ
対称暗号アルゴリズムＦ
暗号文
平　文
暗号化要求電文
[平文＋秘密鍵のＩＤ情報]
暗号化回答電文[暗号文＋ＲＮ]
ホスト側復号化処理
秘密鍵ＳＫ
乱数ＲＮ
対称暗号アルゴリズムＦ
テンポラリ鍵ＴＫ
対称暗号アルゴリズムＦ
暗号文
平　文

【図３】


ICカード10
サービス提供用端末20
ホスト30
ICカード内部復号化処理
秘密鍵SK
乱数RN
暗号文
対称暗号アルゴリズムF
テンポラリ鍵TK
対称暗号アルゴリズムF
平文
復号化要求電文
[暗号文+秘密鍵のID情報+RN]
復号化回答電文[平文]
ホスト側暗号化処理
乱数発生器
乱数RN
対称暗号アルゴリズムF
テンポラリ鍵TK
秘密鍵SK
平文
対称暗号アルゴリズムF
暗号文

【図４】


ＩＣカード
ＩＣカード内部暗号化処理
乱数発生器
乱数ＲＮ
対称暗号アルゴリズムＦ
テンポラリ鍵ＴＫ
秘密鍵ＳＫ
対称暗号アルゴリズムＦ
暗号文
平　文
サービス提供用端末20
暗号化要求電文
[平文＋秘密鍵のＩＤ情報]
暗号化回答電文[暗号文＋ＲＮ]
ホスト30
ホスト側復号化処理
暗号文
秘密鍵ＳＫ
乱数ＲＮ
対称暗号アルゴリズムＦ
テンポラリ鍵ＴＫ
対称暗号アルゴリズムＦ
平　文